

REMARKS

Claims 1, 3, 4, 8, 9, 16, 18, 19, 20, 21, 25 and 29-72 are pending in this application.

Claims 1, 3, 4, 8, 9, 16, 18, 21, and 25 are amended herein. Claims 2, 5, 6, 7, 10-15, 17, 22, 23, 24, 26, 27, and 28 are cancelled herein without prejudice or disclaimer. Claims 29-72 are added herein. Support for the amendments to the claims may be found in the claims as originally filed, as well as in Figs. 21, 24, 27, 29, and 31, and the attendant description. Reconsideration is requested based on the foregoing amendment and the following remarks.

Claim Rejections - 35 U.S.C. § 101:

Claims 1, 3, 4, 8, 9, 16, 18, 19, 20, and 21 were rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter. Claims 1, 3, 4, 8, 9, 16, 18, 19, 20, and 21 were amended to be more tangible.

In any case, 35 U.S.C. § 101, which governs the meaning of statutory subject matter, provides only:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Since the encryption device to which claims 1, 3, 4, 8, 9, 16, 18, 19, 20, and 21 are directed does fall within at least one of the four stated categories of statutory subject matter, i.e. a machine or manufacture, claims 1, 3, 4, 8, 9, 16, 18, 19, 20, and 21 are submitted to be directed to statutory subject matter within the provisions of 35 U.S.C. § 101. Withdrawal of the rejection of claims 3-21 is earnestly solicited.

Claim Rejections - 35 U.S.C. § 112:

Claim 8 was rejected under 35 U.S.C. § 112, second paragraph, as indefinite. Claim 8 was amended to make it more definite. Withdrawal of the rejection is earnestly solicited.

Claim Rejections - 35 U.S.C. § 102:

Claims 1, 3, 4, 8, 9, 16, 18, 19, 20, 21, and 25 were rejected under 35 U.S.C. § 102(b) as anticipated by European Patent Application No. EP 0 981 223 to Kawamura et al. (hereinafter "Kawamura"). The rejection is traversed to the extent it would apply to the claims as amended.

Kawamura describes switching between two sets of fixed mask values and tables for

each process in accordance with a random number. In particular, as described in the Abstract of Kawamura:

A pair of a pattern of a mask (a) and a mask pattern obtained by bit inversion of the mask is prepared for each round function (5) in a data scrambler (1). Every time encryption is to be performed, one mask pattern of the pair is randomly selected by a switch (SW12), and an exclusive OR (32a) of an input to an S-box (29) and the selected mask pattern is calculated. In addition, an exclusive OR (33a) of an output from the S-box (29) and bits of inverse permutation p<-1> of the mask (a) is calculated. The exclusive ORs (32a, 33a) are calculated in advance and stored as a table in the S-box (29). Furthermore, an exclusive OR (43a) of the output from each round function (5) and a mask (b) is calculated and concealed. The influence of the mask (b) is removed by calculating the exclusive OR with the mask (b) again on the next round.

Since Kawamura describes switching between two sets of fixed mask values and tables for each process in accordance with a random number, and the two sets are complements of each other in terms of bits, Kawamura corresponds to the case in the present application in which the number of sets is limited to q=2. This, however, may not be secure depending on the power dissipated by the device, the number of sets of masked values, and the condition of the values. In particular, as described at page 35, lines 7-12 of the specification:

The security against the DPA at the predetermined timing at the measured points B and C shown in FIGURE 9 depends on what model can be used to approximate the relation between the measured voltage and the load value when the value is loaded to the RAM in the encryption processor.

In fact, as shown in Table 2 at page 38 of the present application, the condition of q=2 imposed by Kawamura requires only 2^{23} steps for differential power analysis (DPA), and is consequently not secure. The claimed invention, in contrast, provides higher security for the adjacent bit model than Kawamura, which relates only to the case in which q=2. The claimed invention, furthermore, applies to the cases in which q=2 or $q \geq 3$, and provides heightened security for both. In particular, as recited in claim 1:

q sets of fixed values, where q is equal to two, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0(FMin)$, $C_h = c_{h,15}c_{h,1}\dots c_{h,0}$, and $D_h = d_{h,15}d_{h,14}\dots d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer.

Kawamura neither teaches, discloses, nor suggests "q sets of fixed values, where q is equal to two, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0(FMin)$, $C_h = c_{h,15}c_{h,1}\dots c_{h,0}$, and $D_h = d_{h,15}d_{h,14}\dots d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer," as recited in claim 1.

Claim 1 recites further:

q sets of fixed values, wherein equations, $(c_{0,j} \text{ XOR } c_{1,j}) = (0101\dots01)_2$ or $(1010\dots10)_2$ and $(d_{0,j} \text{ XOR } d_{1,j}) = (0101\dots01)_2$ or $(1010\dots10)_2$ are satisfied, a fixed table before masking is defined as $S[x]$, and i-th masked fixed table is defined as $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$ for the j-th fixed value.

Kawamura neither teaches, discloses, nor suggests "q sets of fixed values, wherein equations, $(c_{0,j} \text{ XOR } c_{1,j}) = (0101\dots01)_2$ or $(1010\dots10)_2$ and $(d_{0,j} \text{ XOR } d_{1,j}) = (0101\dots01)_2$ or $(1010\dots10)_2$ are satisfied, a fixed table before masking is defined as $S[x]$, and i-th masked fixed table is defined as $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$ for the j-th fixed value," as recited in claim 1.

Finally, claim 1 recites:

Linear transform means $L_{1,i}(x)$, and linear transform means $L_{2,i}(x)$, wherein the linear transform means $L_{1,i}(x)$, the nonlinear transform means with the masked fixed table $S_j[x]$ and the linear transform means $L_{2,i}(x)$ operate in i-th one of rounds.

Kawamura neither teaches, discloses, nor suggests "linear transform means $L_{1,i}(x)$, and linear transform means $L_{2,i}(x)$, wherein the linear transform means $L_{1,i}(x)$, the nonlinear transform means with the masked fixed table $S_j[x]$ and the linear transform means $L_{2,i}(x)$ operate in i-th one of rounds," as recited in claim 1. Claim 1 is submitted to be allowable. Withdrawal of the rejection of claim 1 is earnestly solicited.

Claims 3, 4, 8, 9, 16, 18, 19, 20, 21, and 25 recite substantially the above-mentioned limitations, as well as others, and are thus submitted to be allowable as well, for at least those reasons discussed above with respect to claim 1. Withdrawal of the rejection of claims 3, 4, 8, 9, 16, 18, 19, 20, 21, and 25 is earnestly solicited.

New Claims 29-72.

New Claims 29-72 recite substantially the above-mentioned limitations as well, and are thus believed to be allowable.

Conclusion:

Accordingly, in view of the reasons given above, it is submitted that all of claims 1, 3, 4, 8, 9, 16, 18, 19, 20, 21, 25 and 29-72 are allowable over the cited references. Allowance of all claims 1, 3, 4, 8, 9, 16, 18, 19, 20, 21, 25 and 29-72 and of this entire application is therefore respectfully requested.

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Serial No. 10/028,265

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 21 FEB 06

By: 
Thomas E. McKiernan
Registration No. 37,889

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501